UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/822,069	04/09/2004	Jeffrey A. Kraemer	368605	2093

76863 7590 09/30/2008

KRAGULJAC & KALNAY
4700 ROCKSIDE ROAD
SUMMIT ONE, SUITE 510
INDEPENDENCE, OH 44131

EXAMINER	
DOAN, TRANG T	
ART UNIT	PAPER NUMBER
2131	
MAIL DATE	DELIVERY MODE
09/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/822,069	KRAEMER ET AL.	
	Examiner	Art Unit	
	TRANG DOAN	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,5-21,25-41,45-60,81 and 85-98* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,5-21,25-41,45-60,81 and 85-98* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment filed on 07/08/2008.

2. Claims 1, 5, 21, 25, 38, 41, 45, 81, 85 and 96 have been amended.

3. Claims 2-4, 22-24, 42-44, 61-80 and 82-84 have been canceled.

4. Claims 1, 5-21, 25-41, 45-60, 81 and 85-98 are pending for consideration.

Response to Arguments

5. Applicant's argument with respect to the 35 U.S.C. 112, second paragraph, rejection has been fully considered in view of the amendment filed on 07/08/2008, which has been made in record, and the 35 U.S.C. 112, second paragraph, rejection has been withdrawn.

6. Applicant's argument with respect to the 35 U.S.C. 101 rejection has been fully considered in view of the amendment filed on 07/08/2008, which has been made in record, and the 35 U.S.C. 101 rejection has been withdrawn.

7. Applicant's arguments filed on 07/08/2008 have been fully considered but they are not persuasive.

Regarding claims 1, 21, 41 and 81, Applicants submit that Carter fails to teach a time parameter which defines the passage of time perceived by the computer system, the passage of time indicated by the time parameter is faster than the actual passage of time.

Examiner respectfully disagrees with Applicant's argument. Examiner notes, the limitation "the actual passage of time" is not defined in the claims. Examiner does not

know what Applicants mean by that limitation. Examiner will broadly interpret that limitation as best understood. Carter discloses a network surveillance and security system that uses artificial intelligent to model simulations of logical operations involved in securing computers against security threats (Carter: paragraphs 0218, 0256, 0259, 0261, 1100 and 1103). Since the passage of time defined by the time parameter in Carter reference can be changed by a system call, therefore the time parameter is faster than the actual passage of time (Carter: paragraphs 0590, 0595 and 0599).

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Claim Objections

8. Claim 1 is objected to because of the following informalities:

The limitation "in which the reference monitor executes the at least one parameter" should be changed to "in which the reference monitor executes, the at least one parameter".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. Claims 1, 5-21, 25-41, 45-60, 81 and 85-98 are rejected under 35 U.S.C. 102(b) as being anticipated by Carter et al. (US 2003/0051026) (hereinafter Carter).

Regarding claims 1, 21, 41 and 81, Carter discloses:

(A) defining at least one security rule specifying whether to allow or deny a request to access at least one resource under a given set of circumstances (Carter: See Abstract section and paragraphs 0168-0169, 0171, 0258, 0607 and 0802-0803: four sets of policies included in the Network Surveillance and Security System that govern access to databases (i.e., resource));

(B) supplying at least one request to access a resource (Carter: See paragraphs 0180, 0652 and 0755: A Security Reference Monitor is a hidden controller that makes references against the Security Reference Database whenever the Security Reference Monitor detects that the Security Authorization Database receives a request for access); and

(C) applying the at least one security rule in response to the at least one request to access a resource to determine whether to allow or prevent the at least one request (Carter: See paragraphs 0180, 0785 and 0797-0803: the watchdog system may use its

own policies to permit or deny access, or it may pass the decision to other components of the Network Surveillance and Security System); and

providing at least one parameter defining a system environment in which the reference monitor executes, the at least one parameter includes a time parameter which define the passage of time perceived by the computer system, the passage of time indicated by the time parameter is faster than the actual passage time (Carter: paragraphs 0590, 0595 and 0599).

Regarding claims 5, 25, 45 and 85, Carter further discloses wherein the passage of time indicated by the time parameter enables the computer system to execute the reference monitor simulator in an accelerated manner (Carter: See Abstract section and paragraph 0306: the invention autonomously alters its security policies in response to ongoing events).

Regarding claims 6, 26 and 46, Carter further discloses (D) assessing the effectiveness of the at least one security rule (Carter: paragraphs 0222 and 0260).

Regarding claims 7, 27, 47 and 86, Carter further discloses wherein assessing the effectiveness of the security rule further comprises determining at least one of the number of improper access requests prevented and the number of proper access requests allowed (Carter: paragraphs 0260, 0606-0611 and 0802).

Regarding claims 8, 28, 48 and 87, Carter further discloses wherein assessing the effectiveness of the security rule further comprises determining a rate of improper requests prevented (Carter: paragraphs 0403 and 0411-0413).

Regarding claims 9, 29 and 49, Carter further discloses wherein (B) further comprises an application program supplying the at least one request to access a resource (Carter: paragraph 0304).

Regarding claims 10, 30, 50 and 89, Carter further discloses wherein (B) further comprises capturing at least one request to access a resource before supplying the at least one request to access a resource (Carter: paragraphs 0172 and 0218).

Regarding claims 11, 31, 51 and 90, Carter further discloses wherein a reference monitor performs the capture of the at least one request to access a resource (Carter: paragraphs 0700 and 0755).

Regarding claims 12, 32, 52 and 91, Carter further discloses wherein the reference monitor which performs the capture of the at least one request to access a resource is the same type of reference monitor as the reference monitor whose operations are recreated by the reference monitor simulator (Carter: paragraphs 0168-0169, 0180, 0700 and 0755-0756).

Regarding claims 13, 33, 53 and 92, Carter further discloses wherein the captured at least one request to access a resource is an improper request (Carter: paragraphs 0180 and 0222).

Regarding claims 14, 34, 54 and 93, Carter further discloses wherein an improper request comprises a request issued by an application in response to one of a virus and a buffer overrun attack (Carter: paragraphs 0180, 0222 and 0674).

Regarding claims 15, 35, 55 and 94, Carter further discloses wherein the captured at least one request is modified prior to supplying the at least one request to access a resource (Carter: paragraphs 0700 and 0755).

Regarding claims 16, 36, 56 and 95, Carter further discloses wherein the modification is performed by a user (Carter: paragraph 0795).

Regarding claims 17, 37 and 57, Carter further discloses wherein an electronic file system stores the at least one security rule, and wherein (D) further comprises the reference monitor simulator accessing the security rule in the electronic file system in response to receiving the at least one request to access a resource (Carter: paragraphs 0260, 0606-0611 and 0802).

Regarding claims 18, 38, 58 and 96, Carter further discloses wherein the at least one parameter provided to the reference monitor simulator further includes at least one of a system clock, a wrapper function, and a timer event (Carter: paragraph 0880).

Regarding claims 19, 39 and 97, Carter further discloses (E) maintaining statistics on the operation of the reference monitor simulator (Carter: paragraphs 0271 and 0470).

Regarding claims 20, 40, 60 and 98, Carter further discloses wherein the statistics include at least one of the number of requests per resource, number of total requests, type of request per resource, total of each type of request, number of queries, number of callbacks, number of requests allowed compared to number of requests expected, and number of requests prevented compared to number of prevented requests expected (Carter: paragraph 0470).

Regarding claim 88, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2131
/Syed Zia/
Primary Examiner, Art Unit 2131